

STANDARD AGREEMENT

FOR I.T. GOODS/SERVICES ONLY

REGISTRATION NUMBER
08600306113886
PURCHASING AUTHORITY NUMBER
STATE AGENCY NUMBER
05-029
CONTRACTOR NUMBER
05F0055 (EQ)

1. This Agreement is entered into between the State Agency and the Contractor named below

STATE AGENCY'S NAME

BOARD OF EQUALIZATION

(hereafter called State)

CONTRACTOR'S NAME

STEPHEN P. TEALE DATA CENTER

(hereafter called Contractor)

2. The term of this

Agreement is:

07/01/2005

through

06/30/2006

3. The maximum amount

\$ 13,500,000.00

of this Agreement is:

THIRTEEN MILLION FIVE HUNDRED THOUSAND DOLLARS AND 00/100

4. The parties agree to comply with the terms and conditions of the following attachments which are by this reference made a part of the Agreement:

Exhibit A – Statement of Work

1 page

Exhibit B – Budget Detail and Payment Provisions

2 pages

Exhibit C* – General Terms and Conditions

GIA 101

This document can be viewed at: <http://www.ols.dgs.ca.gov/Standard+Language/GIA101.htm>

Exhibit D – Special Terms and Conditions

3 pages

Exhibit E – Alterations to Terms and Conditions (if applicable)

☒ Check box if attached

Exhibit F – Certification of Compliance With Policies

1 page

Exhibit G – Security Compliance Statement

1 page

Exhibit H* – Service Standards and Service Level Objectives

This document can be viewed at: www.teale.ca.gov/resources/slo.pdf

Items shown with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at www.ols.dgs.ca.gov/Standard+Language

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CALIFORNIA
Department of General Services
Use Only

CONTRACTOR'S NAME (If other than an individual, state whether a corporation, partnership, etc.)

STEPHEN P. TEALE DATA CENTER

BY (Authorized Signature)

DATE SIGNED

PRINTED NAME AND TITLE OF PERSON SIGNING

GLEN S. MATSUOKA, ASSISTANT DIRECTOR, ADMINISTRATION DIVISION

ADDRESS

P.O. BOX 1810, RANCHO CORDOVA, CA 95741-1810

STATE OF CALIFORNIA

AGENCY NAME

BOARD OF EQUALIZATION

BY (Authorized Signature)

DATE SIGNED

PRINTED NAME AND TITLE OF PERSON SIGNING

ROBERT SHERBURNE, CONTRACT MANAGER

ADDRESS

450 N STREET, MIC: 24, SACRAMENTO, CA 94279-0024

Agreements over \$50,000 are
exempt from DGS approval per
Delegation DIA-003.

Agreements under \$50,000 are
exempt from DGS approval per
SCM 4.04.5.A.

Item P2.3
3/29/06

Rev. 1, 3/24/06

STATEMENT OF WORK

1. This Interagency Agreement is entered into by and between **BOARD OF EQUALIZATION** (hereinafter referred to as the "State of California" or "Customer") and the Contractor (hereinafter referred to as "Stephen P. Teale Data Center" or "Teale") for the purpose of obtaining information technology services, materials or equipment. This Interagency Agreement specifies by whom the work shall be performed and the time for performance including the date of completion, if applicable. If not set forth in the Interagency Agreement with sufficient specificity, this Interagency Agreement shall be augmented through the Teale Service Request (SR) process with any resulting mutually agreed contractual terms becoming a part of this Interagency Agreement as if fully set forth herein. The Interagency Agreement also provides for payment for these services pursuant to State Administration Manual (SAM) 8752-8752.1 and Section 3.03 of the State Contracting Manual.

2. Teale agrees to:
 - A. Provide efficient and effective services in accordance with Government Code sections 11792-11794, et seq., to the above-named Customer. In addition, Teale is committed to providing a high level of quality service. In order to achieve these goals and to ensure a clear understanding of the Customer's business requirements, Teale provides Customer Representatives to:
 - 1) Maintain a continual working relationship with the Customer.
 - 2) Coordinate joint development of work plans.
 - 3) Develop partnerships to reach shared objectives.
 - B. Teale management is also available to consult with customers in developing strategies for future information technology projects.

3. The contract managers during the term of this Interagency Agreement will be:

STEPHEN P. TEALE DATA CENTER:

CONTRACT ADMINISTRATOR:	CUSTOMER REPRESENTATIVE:
JEANETTE CRISWELL, CONTRACT ANALYST PROCUREMENT SERVICES BRANCH	CUSTOMER RELATIONS BRANCH
P.O. BOX 1810 RANCHO CORDOVA, CA 95741-1810	P.O. BOX 1810 RANCHO CORDOVA, CA 95741-1810
PHONE: (916) 464-4177 FAX (916) 464-4298 EMAIL: JEANETTE.CRISWELL@TEALE.CA.GOV	PHONE: (916) 464-3967 FAX (916) 464-4287

STATE OF CALIFORNIA:

CONTRACT ADMINISTRATOR:	ACCOUNTING CONTACT:
Joyce Lee	Kamaljit Gill
ADDRESS: 450 N STREET, MIC: 24 SACRAMENTO, CA 95814	ADDRESS: 450 N Street, MIC: 23 Sacramento, CA 95814
PHONE: (916) 324-8280 FAX: (916) 322-3184	PHONE: (916) 327-5040 FAX: (916) 464-4287
EMAIL: Joyce.Lee@boe.ca.gov	EMAIL: Kamaljit.Gill@boe.ca.gov

TECHNICAL CONTACT:	ADDITIONAL CONTACT:
Claudia Neal	Sandra Kennedy
ADDRESS: 450 N Street, MIC: 26 Sacramento, CA 95814	ADDRESS: 450 N Street, MIC: 23 Sacramento, CA 95814
PHONE: (916) 323-1671 FAX: (916) 327-3483	PHONE: (916) 327-9629 FAX: (916) 445-2884
EMAIL: Claudia.Neal@boe.ca.gov	EMAIL: Sandra.Kennedy@boe.ca.gov

BUDGET DETAIL AND PAYMENT PROVISIONS

1. GENERAL CUSTOMER OBLIGATIONS

- A. Return completed Fiscal Year Interagency Agreement (IAA) renewal package to Teale no later than June 30, 2005. Services that are provided under the previous year IAA may be terminated as of midnight June 30, 2005, unless the IAA has been received or the Customer has submitted a formal letter of intent to process an IAA to Teale by close of business on June 30, 2005. For IAAs expiring on a date different than Fiscal Year end, the renewal must be received no later than 30 calendar days prior to the expiration date of the IAA. Services provided under the IAA may be terminated as of midnight on the expiration date, unless a formal letter from the Customer stating intent to renew the IAA is received by Teale, by close of business on the expiration date. Any costs incurred by Teale on behalf of the Customer after the expiration date will be billed to the Customer with full payment due within 30 calendar days.
- B. Customers must provide 45 calendar days cancellation notice for specific services to be terminated. Lead-time for cancellation of services is vendor-dependent and may require additional lead-time for processing termination documents. Notification to terminate services must be submitted to Teale via Service Request form (TDC 098). The targeted completion date noted on the Service Request must allow time for the lead-time required to cancel services. Due to the daily accumulation of system utilization and cost activity within the billing system, retroactive termination of services will not be considered. For additional information regarding lead-times for canceling services, please contact your Customer Representative.
- C. Customers are required to submit payments for services billed at the specified rates. Failure to submit payments within 90 calendar days of receipt of invoice constitutes grounds for termination of service. After 90 calendar days, Teale will not process SRs until such time as the Customer has fully paid all outstanding accounts with Teale. Use of services and goods provided by Teale to the Customer constitutes an obligation, which must be paid. Cancellation of service as a result of a lack of payment shall obligate the Customer to return to Teale the products and/or goods supplied pursuant to this IAA at the Customer's sole expense.
- D. In the event the Customer exceeds the amount authorized by this Agreement, the Customer is responsible for all charges incurred, and shall agree to amend this Agreement, in writing, to provide payment to the Teale Data Center to the extent services have been provided. Such payment for services incurred beyond the amount authorized by this Agreement shall be made payable on or before the agreement expiration date. If, after the conclusion of the subject Agreement period, it is determined that monies above and beyond that which was authorized by this Agreement are owed to the Teale Data Center for services received by the Customer, the Customer shall amend the Agreement, agreeing to pay the outstanding amount in full, no later than sixty (60) calendar days from discovery of the outstanding payment due.

2. INVOICING

- A. For services rendered in accordance with this IAA upon receipt of appropriate invoices, the Customer agrees to compensate Teale for actual expenditures incurred in accordance with the rates specified herein.
- B. Invoices shall include the Teale Data Center Interagency Agreement Number and shall be submitted in duplicate not more frequently than monthly in arrears to the accounting contact identified in Exhibit A.

3. BUDGET CONTINGENCY CLAUSE

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Interagency Agreement does not appropriate sufficient funds for the program, this Interagency Agreement shall be of no further force and effect. In this event, the Customer shall have no liability to pay any funds whatsoever to Teale or to furnish any other considerations under this Interagency Agreement, and Teale shall not be obligated to perform any provisions of this Interagency Agreement.
- B. If funding for any Fiscal Year is reduced or deleted by the Budget Act for purposes of this program, the Customer shall have the option to either cancel this Interagency Agreement with no further liability except as otherwise specified herein, or offer an amendment to reflect the reduced amount.

4. PAYMENT TERMS

- A. Costs for this Interagency Agreement shall be computed in accordance with SAM Sections 8752 and 8752.1.
- B. The cost of performance is based upon Teale's Billing Rate Schedule. The rates are subject to change upon 30 calendar days prior written notice from Teale. These rates may be viewed on Teale's web site at: www.teale.ca.gov/services/billing.
- C. Customer agrees to one of the following payment schedules. In the event a payment type is not designated by checking an appropriate box, the payment type will automatically default to Number 1 (Direct Transfer), below.
 - 1) _____ Direct Transfer, or
 - 2) X Customer agrees to pay monthly upon receipt with Teale rendering invoices monthly in arrears to the Customer on a month-to-month basis up to the total amount of this Interagency Agreement.

5. CUSTOMER RESPONSIBILITY

It will be the responsibility of the Customer to notify Teale in writing within five (5) working days after receipt/installation of goods or services from another agency/vendor (i.e., equipment, telecommunication lines, software products). Such notification should be sent to:

Stephen P. Teale Data Center
P.O. Box 1810
Rancho Cordova, CA 95741-1810
Attn: Bureau of Finance/Administrative Services Unit

GIA101 — GENERAL TERMS AND CONDITIONS FOR INTERAGENCY AGREEMENTS

This document can be viewed at: <http://www.ols.dgs.ca.gov/Standard+Language/GIA101.htm>

SPECIAL TERMS AND CONDITIONS

1. AUTHORITY TO ENTER INTO AGREEMENT

Customer hereby warrants and represents that it has the budget and project approvals necessary for Teale services covered under this IAA. Customer further warrants and represents that sufficient monies have been approved by the State or federal governmental agencies, and are available to the Customer to fund the expenditures for Teale services covered under this IAA. Customer acknowledges that it is acting in an independent capacity in signing this IAA and not as agents or employees of Teale.

2. CONFIDENTIALITY

Based on the specific requirements and intent of Government Code sections 11792-11794, et. seq., and sections 4840, et. seq., of the State Administrative Manual, Teale hereby agrees to provide required security to ensure the confidentiality, integrity, availability (within the resources that Teale manages), physical security, and safekeeping of all data, information, files and documents while in its possession. All sensitive data, documentation or other information, which are designated confidential by the Customer and is made available to Teale in order to carry out this IAA, will be protected by Teale from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as used by the Customer. The identification of all such confidential data and information, as well as the Customer's procedural requirements for protection of such data and information from unauthorized use and disclosure, will be provided in writing to Teale by the Customer. Customer will have the opportunity to review, then accept security procedures that are relevant to their data. Upon written request from the Customer, Teale will provide instructions and limited assistance to implement the necessary level of data security without charge. If the Customer does not provide Teale with any unique or special procedural requirements for the protection of its data, the Customer will be deemed to have accepted the security procedures used by Teale. Instructions and/or assistance in excess of four (4) hours in any one (1) month will be charged at the consultant rate itemized in the rate schedule for Teale services.

3. EXAMINATION AND AUDIT

In accordance with Government Code section 8546.7, Teale and the Customer jointly agree that the Bureau of State Audits (BSA) will have the right to review, obtain and copy all records pertaining to performance of the IAA. Teale and Customer agree to provide or otherwise make available to the BSA any relevant information requested and shall permit the BSA access to its premises, upon reasonable notice, during normal business hours for the purpose of interviewing employees and inspecting and copying such books, records, accounts and other material that may be relevant to this IAA. Teale and Customer further agree to maintain such records for a period of three (3) years after final settlement under the IAA.

4. COPYRIGHT INFRINGEMENT

Pursuant to Executive Order D-10-99 and Management Memo 02-16, Customer acknowledges that the use of licensed products in violation of a valid licensing Agreement could subject Teale to third party lawsuits. Therefore, Customer agrees that it will not duplicate, copy or otherwise reproduce any proprietary software products supplied pursuant to this IAA without the express written consent of the owner of the software. Customer further agrees that it will use any such software products in strict compliance with the terms of any license provided by the owner of the software. Customer further agrees that its use of any such licensed software products will not violate any applicable copyright, trademark, trade name, patent or similar legal right.

In the event Teale is sued by a third party as a result of Customer's misuse of any proprietary materials or products supplied under this IAA, Customer agrees to indemnify, defend and hold harmless the Stephen P. Teale Data Center from any and all claims and losses regarding Customer's violation of software licenses, copyrights, trademarks, trade names or any proprietary data, information or materials designated as confidential and supplied under this IAA. If litigation arises as a result of Customer's breach of these obligations, Customer will pay all litigation expenses, including reasonable attorney and expert witness fees (as permitted by law), incurred by Teale in defense or settlement of the legal action or proceeding.

5. UNSUPPORTED SOFTWARE

Teale is not responsible for license, service, and/or support issues related to software in Customer systems, unless Teale is the licensee of the software products. The Customer agrees to maintain appropriate licenses and service and support arrangements for the systems or applications owned or maintained by the Customer's department; all enterprise-wide systems, which include hardware, operating systems; application software (if applicable); security systems; and software licenses for all systems and services. Teale is neither responsible nor liable for damages resulting from the Customer's decision to use unlicensed or unsupported software.

6. LIMITATION OF LIABILITY

Teale shall not be liable for any activity involving Customer's installation of the product, Customer's use of the product, or the results obtained from such use. Teale shall not be liable for any unauthorized access to Customer data or any unauthorized disclosure of Customer data resulting from the Customer's use of any product. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of Teale, its officers, employees or agents.

IN NO EVENT SHALL TEALE BE LIABLE TO THE CUSTOMER FOR CONSEQUENTIAL DAMAGES EVEN IF NOTIFICATION HAS BEEN GIVEN AS TO THE POSSIBILITY OF SUCH DAMAGES.

7. DIGITAL CERTIFICATE SERVICES INDEMNITY

To the extent that this IAA involves digital certificate services, Customer shall be solely liable for any loss, damage or claim of loss or damage resulting from the acquisition, installation, provision or use of any digital certificate services provided by Teale. Customer acknowledges that Teale has made no representations or warranties of any type regarding the use of digital certificates or the possible level of information security provided by such certificates. Customer shall indemnify, defend and hold Teale harmless from any and all claims for invasion of privacy, improper release, dissemination, or distribution of confidential, restricted, defamatory, or proprietary information or data, or any other similar claim for injury or loss, arising from Customer's use of any digital certificate services provided by Teale under this IAA. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of Teale, its officers, employees or agents.

8. VIRTUAL PRIVATE NETWORK SERVICES INDEMNITY

To the extent that this IAA involves Virtual Private Network (VPN) services, Customer shall be solely liable for any loss, damage, or claim of loss or damage resulting from the acquisition, installation, provision or use of any VPN services received under this IAA. Customer acknowledges that Teale has made no representations or warranties of any type regarding the use of VPN or the possible level of information security provided by such VPN. Customer shall indemnify, defend and hold Teale harmless from any and all claims for invasion of privacy, improper release, dissemination, or distribution of confidential, restricted, defamatory, or proprietary information or data, or any other similar claim for injury or loss, arising from Customer's use of any VPN services provided under this IAA. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of Teale, its officers, employees or agents.

9. FUNDING INQUIRY

Teale is required to maintain funding information for federal audit purposes.

- | | | |
|---|---|------------------|
| A. Does your agency receive any federal funds? | Yes <u> X </u> | No <u> </u> |
| B. If yes, does funding for this IAA contain any federal funds? | Yes <u> </u> | No <u> X </u> |
| C. If yes, what dollar amount received by Teale is federal money? | \$ <u> </u> | |
| D. From which fund will the money for this IAA be encumbered? | General <u> X </u> | |
| | Special Fund (specify name of fund) <u> </u> | |
| | Fund Code <u> </u> | |

10. OPERATIONAL RECOVERY INQUIRY

Teale offers Operational Recovery Hot Site Services. Quotations for this service will be provided by Teale's Operational Recovery Coordinator and are based on agency individual requirements.

- | | | |
|---|----------------------------------|------------------|
| A. Does your agency plan to use this service during the term of this Agreement? | Yes <u> X </u> | No <u> </u> |
| B. If yes, are funds included in this IAA for these services? | Yes <u> X </u> | No <u> </u> |
| C. If no, when will the IAA be amended to add funds for these services? | Date <u> </u> | |

In order to provide for the emergency restoration of Customer's systems in the event of a disaster, Customer must separately subscribe to the Operational Recovery Services offered by the Teale Data Center. If Customer has not subscribed to these Operational Recovery Services, Customer's operations may not be restored for a significant length of time and Teale will not be responsible for the proper operation of Customer's systems in the event of a disaster.

11. RETENTION AND PURGING OF ELECTRONIC DATA FOR PURPOSES OF DISCOVERY

The Customer shall contact the Teale Data Center, in writing, with instructions regarding the retention and purging of electronic data. As the repository of the Customer's electronic data, Teale Data Center has no control over the retention and purging of said data, beyond that which the Customer specifically directs.

Should the Customer become involved in litigation, or the Customer informs Teale that litigation is reasonably foreseeable and that all electronic data from that point forward must be retained (and/or any previous electronic data restored), it is the Customer's sole responsibility to give written instructions to Teale including, but not limited to, a clear and concise description of the data to be stored; the manner in which the electronic data is to be stored; the period for which the electronic data is to be stored, and whether or not back up tapes are to be made. Further, it is the Customer's sole responsibility to contact Teale, in writing, and advise when said documentation is to be destroyed. Upon completion of said purging, Teale shall send a letter to the Customer confirming destruction of the described data.

Should the Customer's electronic data be subject to a Public Records Act (PRA) request to produce electronic data or to produce documents in an electronic format it is, as set forth in Government Code section 6250 et. seq., the Customer's sole responsibility to communicate with the requestor, and to produce said documents at its own costs and expense. It is in the Customer's discretion to determine if Teale's services are desired or necessary to extract information responsive to the PRA request that may be stored electronically and, therefore, to retain Teale for such services in a separate agreement.

12. DATA CENTER CONSOLIDATION

Customer acknowledges that Teale Data Center ("Teale") may be legislatively mandated to consolidate the operation of its data center with the State of California, Health and Human Services Data Center ("HHSDC") and/or other state entities with whom Contractor contracts, and not as a matter of convenience. All Customer contracts with Teale and with HHSDC may be consolidated to a single contract for purposes of administrative efficiency through amendment.

ALTERATIONS TO IAA – STD 213 TERMS AND CONDITIONS

Add the following sentence within Exhibit D, Page 1 of 3, Item 2, Confidentiality, at the end of the paragraph:

The provisions of Exhibit E to this interagency agreement constitute the BOE's written request specifying BOE's special procedural requirements for the protection of federal tax information from unauthorized disclosure and use.

**COMPLIANCE WITH MANDATORY FEDERAL LAW REQUIREMENTS
FOR SAFEGUARDING FEDERAL TAX INFORMATION**

The Department of Technology Services (DTS) agrees to adhere to the requirements of section 6103(n) of the Internal Revenue Code, and as set forth in Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, section 5.5 and Exhibit 5. IRC section 6103(n) authorizes a state tax agency, such as the Board of Equalization, to disclose federal tax information (FTI) to "any other person" to the extent necessary in connection with the contractual procurement of services, equipment or other property for tax administration purposes. The phrase, "any other person," means a state government agency such as the DTS as well as any private firm providing services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes. (26 CFR §301.6103(n)-1(a)(2).)

1. The Board of Equalization (BOE) receives, processes, stores and transmits FTI for tax administration purposes, as authorized by the "Agreement on Coordination of Tax Administration between the Board of Equalization and the Internal Revenue Service," effective April 17, 1997, and updated "Memorandum of Implementation," effective July 7, 2004. These agreements require the BOE to adhere to the requirements of section 6103 of the Internal Revenue Code, to ensure the confidentiality of returns and return information. IRC § 6103 requires the BOE to have adequate programs in place involving policies, practices, controls and safeguards, to protect the FTI data from unauthorized use, access and disclosure within the BOE, as well as within the DTS, as an agency-shared facility providing data processing services to the BOE.
2. IRC § 6103(n) requires the BOE to include in this interagency agreement (Agreement) with the DTS for data processing services, the requirements set forth in Exhibit 5 of the Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.
3. An additional requirement of IRC § 6103(n) is that the BOE is to make periodic inspections of the DTS, since it is an agency-shared data center serving numerous state agencies, and to keep a written record of such inspections. The DTS is also subject to site inspections conducted by the Internal Revenue Service (IRS) to ensure that adequate safeguards are in place to protect the BOE's FTI data from unauthorized use, access and disclosure. (See page 4 of this Exhibit.)

4. The above-stated requirements of IRC § 6103(n) also apply when magnetic media containing FTI is released to a private contractor. The DTS contracts with Iron Mountain Off-Site Data Protection which, on behalf of the DTS, provides off-site data storage for the BOE's magnetic media and/or documents containing FTI. The DTS agrees to adhere to section 6103(n) requirements to include the IRS requirements for safeguarding FTI in its 2006-2007 Agreement with Iron Mountain, on behalf of the BOE, for storage of BOE's magnetic media containing FTI, as set forth in Exhibit 5 of the Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.
5. The DTS acknowledges that Iron Mountain, which receives and stores magnetic media and/or documents containing the BOE's FTI, is subject to periodic site inspections conducted by both the BOE and the Internal Revenue Service (IRS) to ensure that adequate safeguards are in place to protect the FTI from unauthorized use, access and disclosure. (See page 4 of this Exhibit.)
6. The DTS agrees that the above-stated requirements of IRC § 6103(n) apply to any private contractor with whom it contracts to provide Operational Recovery Hot Site Services to the BOE since that contractor is to receive magnetic media containing FTI from the BOE.
7. The DTS agrees that the above-stated requirements of IRC § 6103(n) apply to any private contractor with whom it contracts for services on behalf of the BOE that will receive magnetic media containing FTI.

I. PERFORMANCE

In the performance of this Agreement between the BOE and the DTS, the Contractor (DTS) agrees to comply with and assume responsibility for compliance by the DTS' employees with the following requirements:

1. All work will be done under the supervision of the DTS or its employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Agreement and except as authorized by federal and state statutory law. Disclosure to anyone other than an officer or employee of the DTS will be prohibited. To the extent that other types of information held by the BOE are open to disclosure under federal or state law, the BOE agrees to provide such information in response to, but not limited to, court orders, Public Records Act requests and investigations by law enforcement authorities. (See Special Terms and Conditions, Exhibit D, number 11.)

3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. The DTS certifies that the data processed during the performance of this Agreement will be completely purged from all data storage components of the DTS' computer facility, and no output will be retained by the DTS at the time the work is completed. If immediate purging of all data storage components is not possible, the DTS certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the BOE's specified designee(s). When this is not possible, the DTS will be responsible for the destruction of the spoilage or any intermediate hardcopy printouts, and will provide to the BOE's specified designee(s) with a statement containing the date of destruction, description of material destroyed and the method used.
6. All computer systems processing, storing, or transmitting Federal tax information must meet the federal standard for security features, Common Criteria for Information Technology Security Evaluation, usually referred to as the Common Criteria, ISO STD 15408. To meet functional and assurance requirements of this standard, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
7. No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
8. The DTS will maintain a list of employees with authorized access. Such list will be provided to the BOE and, upon request, to the IRS reviewing office.
9. The BOE will have the right to void this Agreement if the DTS fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of the DTS to whom returns or return information is or may be disclosed will be notified in writing by the DTS that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as

long as 5 years, or both, together with the costs of prosecution. The DTS shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC §§ 7213 and 7431 and set forth at 26 CFR 301.6103(n).

2. Each officer or employee of the DTS to whom returns or return information is or may be disclosed shall be notified in writing by the DTS that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. The DTS shall also notify such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC §§ 7213A and 7431.
3. Additionally, it is incumbent upon the DTS to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to the DTS by U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

III. INSPECTION

The IRS and the BOE each shall have the right to send its specifically-authorized officers and employees into the offices and plants of the DTS for inspection of the facilities and operations provided for the performance of any work under this Agreement. On the basis of such inspection, specific measures may be required in cases where the DTS is found to be noncompliant with contract safeguards. The DTS agrees to allow an annual site inspection for this purpose by the BOE's specifically-authorized employees and, upon request, by the IRS, and to facilitate an annual site inspection of the Iron Mountain storage facility conducted by the BOE's specifically-authorized employees and, upon request, by the IRS.

CERTIFICATION REQUIREMENTS

4832 Illustration 1

CERTIFICATION OF COMPLIANCE WITH POLICIES

Pursuant to SAM Section 4819.41 and 4832

I hereby certify that I am the agency director or designee; that the matters described herein are in compliance with the criteria and procedures for information technology prescribed in State Administrative Manual (SAM); any acquisitions of new or enhanced information technology capabilities are consistent with project justification approved by Department of Finance, myself or my designee; and that the foregoing statements are true to the best of my knowledge and belief.

7/6/05

Date

Carol L. L. L. L.

Signature and Title
(Specify director or designee)

JUSTIFICATION AND APPROVAL REFERENCE INFORMATION

Finance-Approved FSR

Finance Project #

Approval Date

Agency-Approved FSR

Agency Project #

Approval Date

Workgroup Computing
Justification Form (WCJP)

WCJF #

Approval Date

Project Title

X

Data Center IAA - This is an Interagency Agreement to procure services from a consolidated data center; it involves multiple projects; the funding level is appropriate, and the nature and scope of services to be supplied by the Data Center are consistent with the various approved FSRs and PIERs of this agency; and the required project reporting associated with each active project is current.

SECURITY COMPLIANCE STATEMENT

Teale Data Center provides for the integrity and security of customer information assets and complies with the policies as set forth in the State Administrative Manual sections 4840-4845. Entities requesting to connect their networks or their network devices to Teale network or resources accessible on Teale's network, must comply with the following basic information security requirements. These requirements will be included in any Agreement or contract with an entity that includes the provision of connectivity to Teale or a resource accessible on Teale's network.

A. Firewalls - This requirement provides a reliable mechanism to help protect Teale and its customers' information and information processing resources from unauthorized access to, and denial/disruption of services or systems.

- **Definition** - A firewall is a computer or system of computers designed to restrict network traffic in order to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, but are strongest when implemented as a hardware/software combination.
- **Requirements** - Any network used by a customer to connect to Teale information resources will be protected by at least one firewall system properly situated to examine traffic between the network and each external network entry point. The customer shall ensure that firewalls include, at a minimum, provisions for packet filtering, application gateway security mechanisms, and circuit-level gateways.

B. Physical Security - This requirement ensures that the hardware that permits network access to Teale Data Center is adequately protected to prevent harm to the physical components that enable connectivity between the customer's network and Teale Data Center.

- **Definition** - Physical Security involves measures taken to prevent physical access, which may allow loss of or damage to, the system or the information stored on it.
- **Requirements** - Physical access to network components, servers, and data storage components used in conjunction with access to Teale Data Center information resources should be limited to the appropriate designated staff who implement and maintain the components.

C. Access Control - This requirement ensures that policies, procedures and technology mechanisms are in place for Teale's customers only to limit access to the Teale Data Center's network and the information resources in Teale's custody to those authorized individuals or entities.

- **Definition** - Access control includes processes and systems to determine which system resources, application functions and information must be restricted to certain customers, business partners, and contractors and to allow access by those customers while preventing access by others.
- **Requirements** - Access to information designated as private or confidential must be limited to those individuals or entities specifically authorized to access that information. Access to system functions and processes under Teale Data Center's custody that can affect the availability, functionality or security of departmental information or information resources should be restricted to those individuals who require that access in order to perform duties essential to the operation and maintenance or use of that system.

Teale is requiring Security Compliance for audit purposes.

- ☒ Customer is in full compliance with the aforementioned security requirements.
- ☐ Customer is not in full compliance, however, will contact Teale's Information Security Officer at (916) 464-3672 to develop a plan of action for compliance with the security requirements.
- ☐ Not Applicable - Customer does not have a network connection to Teale Data Center.

Stephanie Cwardes
Information Security Officer Signature

6-29-05
Date

SERVICE STANDARDS AND SERVICE LEVEL OBJECTIVES

This document can be viewed on Teale's web page at: www.teale.ca.gov/resources/slo.pdf

STANDARD AGREEMENT

FOR I.T. GOODS/SERVICES ONLY

REGISTRATION NUMBER

PURCHASING AUTHORITY NUMBER

STATE AGENCY NUMBER

06-063

CONTRACTOR NUMBER

1. This Agreement is entered into between the State Agency and the Contractor named below

STATE AGENCY'S NAME

BOARD OF EQUALIZATION

(hereafter called State)

CONTRACTOR'S NAME

DEPARTMENT OF TECHNOLOGY SERVICES

(hereafter called Contractor)

2. The term of this Agreement is: 07/01/2006 through 06/30/2007

3. The maximum amount \$ 13,500,000.00
of this Agreement is: THIRTEEN MILLION FIVE HUNDRED THOUSAND DOLLARS AND NO CENTS.

4. The parties agree to comply with the terms and conditions of the following attachments which are by this reference made a part of the Agreement:

Exhibit A – Statement of Work 1 page
Exhibit B – Budget Detail and Payment Provisions 2 pages
Exhibit C* – General Terms and Conditions GIA 101

This document can be viewed at: <http://www.ols.dgs.ca.gov/Standard+Language/GIA101.htm>

Exhibit D – Special Terms and Conditions 3 pages

Exhibit E – Alterations to Terms and Conditions (if applicable) ☒ Check box if attached

Exhibit F – Certification of Compliance With Policies 1 page

Exhibit G – Security Compliance Statement 1 page

Exhibit H* – Service Standards and Service Level Objectives

This document can be viewed at: www.DTS.ca.gov/resources/slo.pdf

Items shown with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at www.ols.dgs.ca.gov/Standard+Language

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CALIFORNIA
Department of General Services
Use Only

CONTRACTOR'S NAME (If other than an individual, state whether a corporation, partnership, etc.)

DEPARTMENT OF TECHNOLOGY SERVICES

BY (Authorized Signature)

DATE SIGNED

PRINTED NAME AND TITLE OF PERSON SIGNING

GLEN S. MATSUOKA, Assistant Director, Administration Division

ADDRESS

P.O. Box 1810, Rancho Cordova, CA 95741-1810

STATE OF CALIFORNIA

AGENCY NAME

BOARD OF EQUALIZATION

BY (Authorized Signature)

DATE SIGNED

PRINTED NAME AND TITLE OF PERSON SIGNING

Barbara Gilbertson, Contract Manager

ADDRESS

Agreements over \$50,000 are exempt from DGS approval per Delegation DIA-003.

Agreements under \$50,000 are exempt from DGS approval per SCM 4.04.5.A.

STATEMENT OF WORK

1. This Interagency Agreement is entered into by and between **BOARD OF EQUALIZATION** (hereinafter referred to as the "State of California" or "Customer") and the Contractor (hereinafter referred to as "DEPARTMENT OF TECHNOLOGY SERVICES" or "DTS") for the purpose of obtaining information technology services, materials or equipment. This Interagency Agreement specifies by whom the work shall be performed and the time for performance including the date of completion, if applicable. If not set forth in the Interagency Agreement with sufficient specificity, this Interagency Agreement shall be augmented through the DTS Service Request (SR) process with any resulting mutually agreed contractual terms becoming a part of this Interagency Agreement as if fully set forth herein. The Interagency Agreement also provides for payment for these services pursuant to State Administration Manual (SAM) 8752-8752.1 and Section 3.03 of the State Contracting Manual.

2. DTS agrees to:
 - A. Provide efficient and effective services in accordance with Government Code sections 11792-11794, et seq., to the above-named Customer. In addition, DTS is committed to providing a high level of quality service. In order to achieve these goals and to ensure a clear understanding of the Customer's business requirements, DTS provides Customer Representatives to:
 - 1) Maintain a continual working relationship with the Customer.
 - 2) Coordinate joint development of work plans.
 - 3) Develop partnerships to reach shared objectives.
 - B. DTS management is also available to consult with customers in developing strategies for future information technology projects.

3. The contract managers during the term of this Interagency Agreement will be:

DEPARTMENT OF TECHNOLOGY SERVICES :

CONTRACT ADMINISTRATOR:	CUSTOMER REPRESENTATIVE:
JEANETTE CRISWELL, CONTRACT ANALYST PROCUREMENT SERVICES BRANCH	CUSTOMER RELATIONS BRANCH
P.O. BOX 1810 RANCHO CORDOVA, CA 95741-1810	P.O. BOX 1810 RANCHO CORDOVA, CA 95741-1810
PHONE: (916) 464-4177 FAX (916) 464-4298 EMAIL: JEANETTE.CRISWELL@DTS.CA.GOV	PHONE: (916) 464-3967 FAX (916) 464-4287

STATE OF CALIFORNIA:

CONTRACT ADMINISTRATOR:	ACCOUNTING CONTACT:
Joyce Lee	Amber Adge
ADDRESS: 450 N STREET, MIC: 24 SACRAMENTO, CA 95814	ADDRESS: 450 N Street, MIC: 23 Sacramento, CA 95814
PHONE: (916) 324-8280 FAX: (916) 322-3184 EMAIL: Joyce.Lee@boe.ca.gov	PHONE: (916) 327-2046 FAX: (916) 464-4287 EMAIL: Amber.Adge@boe.ca.gov

TECHNICAL CONTACT:	ADDITIONAL CONTACT:
Claudia Neal	Sandra Kennedy
ADDRESS: 450 N Street, MIC: 26 Sacramento, CA 95814	ADDRESS: 450 N Street, MIC:23 Sacramento, CA 95814
PHONE: (916) 323-1671 FAX: (916) 327-3483 EMAIL: Claudia.Neal@boe.ca.gov	PHONE: (916) 327-9629 FAX: (916) 445-2884 EMAIL: Sandra.Kennedy@boe.ca.gov

BUDGET DETAIL AND PAYMENT PROVISIONS

1. GENERAL CUSTOMER OBLIGATIONS

- A. Return completed Fiscal Year Interagency Agreement (IAA) renewal package to DTS no later than June 30, 2006. Services that are provided under the previous year IAA may be terminated as of midnight June 30, 2006, unless the IAA has been received or the Customer has submitted a formal letter of intent to process an IAA to DTS by close of business on June 30, 2006. For IAAs expiring on a date different than Fiscal Year end, the renewal must be received no later than 30 calendar days prior to the expiration date of the IAA. Services provided under the IAA may be terminated as of midnight on the expiration date, unless a formal letter from the Customer stating intent to renew the IAA is received by DTS, by close of business on the expiration date. Any costs incurred by DTS on behalf of the Customer after the expiration date will be billed to the Customer with full payment due within 30 calendar days.
- B. Customers must provide 45 calendar days cancellation notice for specific services to be terminated. Lead-time for cancellation of services is vendor-dependent and may require additional lead-time for processing termination documents. Notification to terminate services must be submitted to DTS via Service Request form (TDC 098). The targeted completion date noted on the Service Request must allow time for the lead-time required to cancel services. Due to the daily accumulation of system utilization and cost activity within the billing system, retroactive termination of services will not be considered. For additional information regarding lead-times for canceling services, please contact your Customer Representative.
- C. Customers are required to submit payments for services billed at the specified rates. Failure to submit payments within 90 calendar days of receipt of invoice constitutes grounds for termination of service. After 90 calendar days, DTS will not process SRs until such time as the Customer has fully paid all outstanding accounts with DTS. Use of services and goods provided by DTS to the Customer constitutes an obligation, which must be paid. Cancellation of service as a result of a lack of payment shall obligate the Customer to return to DTS the products and/or goods supplied pursuant to this IAA at the Customer's sole expense.
- D. In the event the Customer exceeds the amount authorized by this Agreement, the Customer is responsible for all charges incurred, and shall agree to amend this Agreement, in writing, to provide payment to the DTS to the extent services have been provided. Such payment for services incurred beyond the amount authorized by this Agreement shall be made payable on or before the agreement expiration date. If, after the conclusion of the subject Agreement period, it is determined that monies above and beyond that which was authorized by this Agreement are owed to the DTS for services received by the Customer, the Customer shall amend the Agreement, agreeing to pay the outstanding amount in full, no later than sixty (60) calendar days from discovery of the outstanding payment due.

2. INVOICING

- A. For services rendered in accordance with this IAA upon receipt of appropriate invoices, the Customer agrees to compensate DTS for actual expenditures incurred in accordance with the rates specified herein.
- B. Invoices shall include the DTS Interagency Agreement Number and shall be submitted in duplicate not more frequently than monthly in arrears to the accounting contact identified in Exhibit A.

3. BUDGET CONTINGENCY CLAUSE

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Interagency Agreement does not appropriate sufficient funds for the program, this Interagency Agreement shall be of no further force and effect. In this event, the Customer shall have no liability to pay any funds whatsoever to DTS or to furnish any other considerations under this Interagency Agreement, and DTS shall not be obligated to perform any provisions of this Interagency Agreement.
- B. If funding for any Fiscal Year is reduced or deleted by the Budget Act for purposes of this program, the Customer shall have the option to either cancel this Interagency Agreement with no further liability except as otherwise specified herein, or offer an amendment to reflect the reduced amount.

4. PAYMENT TERMS

- A. Costs for this Interagency Agreement shall be computed in accordance with SAM Sections 8752 and 8752.1.
- B. The cost of performance is based upon DTS's Billing Rate Schedule. The rates are subject to change upon 30 calendar days prior written notice from DTS. These rates may be viewed on DTS's web site at: www.DTS.ca.gov/services/billing.
- C. Customer agrees to one of the following payment schedules. In the event a payment type is not designated by checking an appropriate box, the payment type will automatically default to Number 1 (Direct Transfer), below.
- 1) _____ Direct Transfer, or
- 2) X Customer agrees to pay monthly upon receipt with DTS rendering invoices monthly in arrears to the Customer on a month-to-month basis up to the total amount of this Interagency Agreement.

5. CUSTOMER RESPONSIBILITY

It will be the responsibility of the Customer to notify DTS in writing within five (5) working days after receipt/installation of goods or services from another agency/vendor (i.e., equipment, telecommunication lines, software products). Such notification should be sent to:

Department of Technology Services
P.O. Box 1810
Rancho Cordova, CA 95741-1810
Attn: Bureau of Finance/Administrative Services Unit

GIA101 — GENERAL TERMS AND CONDITIONS FOR INTERAGENCY AGREEMENTS

This document can be viewed at: <http://www.ols.dgs.ca.gov/Standard+Language/GIA101.htm>

SPECIAL TERMS AND CONDITIONS

1. AUTHORITY TO ENTER INTO AGREEMENT

Customer hereby warrants and represents that it has the budget and project approvals necessary for DTS services covered under this IAA. Customer further warrants and represents that sufficient monies have been approved by the state or federal governmental agencies, and are available to the Customer to fund the expenditures for DTS services covered under this IAA. Customer acknowledges that it is acting in an independent capacity in signing this IAA and not as agents or employees of DTS.

2. CONFIDENTIALITY

Based on the specific requirements and intent of Government Code sections 11792-11794, et seq., and sections 4840, et seq., of the State Administrative Manual, DTS hereby agrees to provide required security to ensure the confidentiality, integrity, availability (within the resources that DTS manages), physical security, and safekeeping of all data, information, files and documents while in its possession. All sensitive data, documentation or other information, which are designated confidential by the Customer and is made available to DTS in order to carry out this IAA, will be protected by DTS from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as used by the Customer. The identification of all such confidential data and information, as well as the Customer's procedural requirements for protection of such data and information from unauthorized use and disclosure, will be provided in writing to DTS by the Customer. Customer will have the opportunity to review, then accept security procedures that are relevant to their data. Upon written request from the Customer, DTS will provide instructions and limited assistance to implement the necessary level of data security without charge. If the Customer does not provide DTS with any unique or special procedural requirements for the protection of its data, the Customer will be deemed to have accepted the security procedures used by DTS. Instructions and/or assistance in excess of four (4) hours in any one month will be charged at the consultant rate itemized in the rate schedule for DTS services. The provisions of Exhibit E to this interagency agreement constitute the BOE's written request specifying BOE's special procedural requirements for the protection of federal tax information from unauthorized disclosure and use.

3. EXAMINATION AND AUDIT

In accordance with Government Code section 8546.7, DTS and the Customer jointly agree that the Bureau of State Audits (BSA) will have the right to review, obtain and copy all records pertaining to performance of the IAA. DTS and Customer agree to provide or otherwise make available to the BSA any relevant information requested and shall permit the BSA access to its premises, upon reasonable notice, during normal business hours for the purpose of interviewing employees and inspecting and copying such books, records, accounts and other material that may be relevant to this IAA. DTS and Customer further agree to maintain such records for a period of three (3) years after final settlement under the IAA.

4. COPYRIGHT INFRINGEMENT

Pursuant to Executive Order D-10-99 and Management Memo 02-16, Customer acknowledges that the use of licensed products in violation of a valid licensing Agreement could subject DTS to third party lawsuits. Therefore, Customer agrees that it will not duplicate, copy or otherwise reproduce any proprietary software products supplied pursuant to this IAA without the express written consent of the owner of the software. Customer further agrees that it will use any such software products in strict compliance with the terms of any license provided by the owner of the software. Customer further agrees that its use of any such licensed software products will not violate any applicable copyright, trademark, trade name, patent or similar legal right.

In the event DTS is sued by a third party as a result of Customer's misuse of any proprietary materials or products supplied under this IAA, Customer agrees to indemnify, defend and hold harmless the DTS from any and all claims and losses regarding Customer's violation of software licenses, copyrights, trademarks, trade names or any proprietary data, information or materials designated as confidential and supplied under this IAA. If litigation arises as a result of Customer's breach of these obligations, Customer will pay all litigation expenses, including reasonable attorney and expert witness fees (as permitted by law), incurred by DTS in defense or settlement of the legal action or proceeding.

5. UNSUPPORTED SOFTWARE

DTS is not responsible for license, service, and/or support issues related to software in Customer systems, unless DTS is the licensee of the software products. The Customer agrees to maintain appropriate licenses and service and support arrangements for the systems or applications owned or maintained by the Customer's department; all enterprise-wide systems, which include hardware, operating systems; application software (if applicable); security systems; and software licenses for all systems and services. DTS is neither responsible nor liable for damages resulting from the Customer's decision to use unlicensed or unsupported software.

6. LIMITATION OF LIABILITY

DTS shall not be liable for any activity involving Customer's installation of the product, Customer's use of the product, or the results obtained from such use. DTS shall not be liable for any unauthorized access to Customer data or any unauthorized disclosure of Customer data resulting from the Customer's use of any product. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of DTS, its officers, employees or agents.

IN NO EVENT SHALL DTS BE LIABLE TO THE CUSTOMER FOR CONSEQUENTIAL DAMAGES EVEN IF NOTIFICATION HAS BEEN GIVEN AS TO THE POSSIBILITY OF SUCH DAMAGES.

7. DIGITAL CERTIFICATE SERVICES INDEMNITY

To the extent that this IAA involves digital certificate services, Customer shall be solely liable for any loss, damage or claim of loss or damage resulting from the acquisition, installation, provision or use of any digital certificate services provided by DTS. Customer acknowledges that DTS has made no representations or warranties of any type regarding the use of digital certificates or the possible level of information security provided by such certificates. Customer shall indemnify, defend and hold DTS harmless from any and all claims for invasion of privacy, improper release, dissemination, or distribution of confidential, restricted, defamatory, or proprietary information or data, or any other similar claim for injury or loss, arising from Customer's use of any digital certificate services provided by DTS under this IAA. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of DTS, its officers, employees or agents.

8. VIRTUAL PRIVATE NETWORK SERVICES INDEMNITY

To the extent that this IAA involves Virtual Private Network (VPN) services, Customer shall be solely liable for any loss, damage, or claim of loss or damage resulting from the acquisition, installation, provision or use of any VPN services received under this IAA. Customer acknowledges that DTS has made no representations or warranties of any type regarding the use of VPN or the possible level of information security provided by such VPN. Customer shall indemnify, defend and hold DTS harmless from any and all claims for invasion of privacy, improper release, dissemination, or distribution of confidential, restricted, defamatory, or proprietary information or data, or any other similar claim for injury or loss, arising from Customer's use of any VPN services provided under this IAA. The limitation of liability provided for by this section shall not apply to any unauthorized access to Customer data or any unauthorized disclosure of Customer data that is caused by the negligent or intentional misconduct of DTS, its officers, employees or agents.

9. FUNDING INQUIRY

DTS is required to maintain funding information for federal audit purposes.

- | | | |
|---|---|----------------------|
| A. Does your agency receive any federal funds? | Yes <u> x </u> | No <u> </u> |
| B. If yes, does funding for this IAA contain any federal funds? | Yes <u> </u> | No <u> x </u> |
| C. If yes, what dollar amount received by DTS is federal money? | \$ <u> </u> | |
| D. From which fund will the money for this IAA be encumbered? | General <u> x </u> | |
| | Special Fund (specify name of fund) <u> </u> | |
| | Fund Code <u> </u> | |

10. OPERATIONAL RECOVERY INQUIRY

DTS offers Operational Recovery Hot Site Services. Quotations for this service will be provided by DTS's Operational Recovery Coordinator and are based on agency individual requirements.

- | | | |
|---|--|----------------------|
| A. Does your agency plan to use this service during the term of this Agreement? | Yes <u> x </u> | No <u> </u> |
| B. If yes, are funds included in this IAA for these services? | Yes <u> x </u> | No <u> </u> |
| C. If no, when will the IAA be amended to add funds for these services? | Date <u> </u> | |

In order to provide for the emergency restoration of Customer's systems in the event of a disaster, Customer must separately subscribe to the Operational Recovery Services offered by the DTS. If Customer has not subscribed to these Operational Recovery Services, Customer's operations may not be restored for a significant length of time and DTS will not be responsible for the proper operation of Customer's systems in the event of a disaster.

11. RETENTION AND PURGING OF ELECTRONIC DATA FOR PURPOSES OF DISCOVERY

The Customer shall contact the DTS, in writing, with instructions regarding the retention and purging of electronic data. As the repository of the Customer's electronic data, DTS has no control over the retention and purging of said data, beyond that which the Customer specifically directs.

Should the Customer become involved in litigation, or the Customer informs DTS that litigation is reasonably foreseeable and that all electronic data from that point forward must be retained (and/or any previous electronic data restored), it is the Customer's sole responsibility to give written instructions to DTS including, but not limited to, a clear and concise description of the data to be stored; the manner in which the electronic data is to be stored; the period for which the electronic data is to be stored, and whether or not back up tapes are to be made. Further, it is the Customer's sole responsibility to contact DTS, in writing, and advise when said documentation is to be destroyed. Upon completion of said purging, DTS shall send a letter to the Customer confirming destruction of the described data.

Should the Customer's electronic data be subject to a Public Records Act request to produce electronic data or to produce documents in an electronic format it is, as set forth in Government Code section 6250 et. seq., the Customer's sole responsibility to communicate with the requestor, and to produce said documents at its own costs and expense. It is in the Customer's discretion to determine if DTS's services are desired or necessary to extract information responsive to the PRA request that may be stored electronically and, therefore, to retain DTS for such services in a separate agreement.

ALTERATIONS TO IAA – STD 213 TERMS AND CONDITIONS

**COMPLIANCE WITH MANDATORY FEDERAL LAW REQUIREMENTS
FOR SAFEGUARDING FEDERAL TAX INFORMATION**

The Department of Technology Services (DTS) agrees to adhere to the requirements of section 6103(n) of the Internal Revenue Code, and as set forth in Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, section 5.5 and Exhibit 5. IRC section 6103(n) authorizes a state tax agency, such as the Board of Equalization, to disclose federal tax information (FTI) to “any other person” to the extent necessary in connection with the contractual procurement of services, equipment or other property for tax administration purposes. The phrase, “any other person,” means a state government agency such as the DTS as well as any private firm providing services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes. (26 CFR §301.6103(n)-1(a)(2).)

1. The Board of Equalization (BOE) receives, processes, stores and transmits FTI for tax administration purposes, as authorized by the “Agreement on Coordination of Tax Administration between the Board of Equalization and the Internal Revenue Service,” effective April 17, 1997, and updated “Memorandum of Implementation,” effective July 7, 2004. These agreements require the BOE to adhere to the requirements of section 6103 of the Internal Revenue Code, to ensure the confidentiality of returns and return information. IRC § 6103 requires the BOE to have adequate programs in place involving policies, practices, controls and safeguards, to protect the FTI data from unauthorized use, access and disclosure within the BOE, as well as within the DTS, as an agency-shared facility providing data processing services to the BOE.
2. IRC § 6103(n) requires the BOE to include in this interagency agreement (Agreement) with the DTS for data processing services, the requirements set forth in Exhibit 5 of the Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.
3. An additional requirement of IRC § 6103(n) is that the BOE is to make periodic inspections of the DTS, since it is an agency-shared data center serving numerous state agencies, and to keep a written record of such inspections. The DTS is also subject to site inspections conducted by the Internal Revenue Service (IRS) to ensure that adequate safeguards are in place to protect the BOE’s FTI data from unauthorized use, access and disclosure. (See page 4 of this Exhibit.)

4. The above-stated requirements of IRC § 6103(n) also apply when magnetic media containing FTI is released to a private contractor. The DTS contracts with Iron Mountain Off-Site Data Protection which, on behalf of the DTS, provides off-site data storage for the BOE's magnetic media and/or documents containing FTI. The DTS agrees to adhere to section 6103(n) requirements to include the IRS requirements for safeguarding FTI in its 2006-2007 Agreement with Iron Mountain, on behalf of the BOE, for storage of BOE's magnetic media containing FTI, as set forth in Exhibit 5 of the Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.
5. The DTS acknowledges that Iron Mountain, which receives and stores magnetic media and/or documents containing the BOE's FTI, is subject to periodic site inspections conducted by both the BOE and the Internal Revenue Service (IRS) to ensure that adequate safeguards are in place to protect the FTI from unauthorized use, access and disclosure. (See page 4 of this Exhibit.)
6. The DTS agrees that the above-stated requirements of IRC § 6103(n) apply to any private contractor with whom it contracts to provide Operational Recovery Hot Site Services to the BOE since that contractor is to receive magnetic media containing FTI from the BOE.
7. The DTS agrees that the above-stated requirements of IRC § 6103(n) apply to any private contractor with whom it contracts for services on behalf of the BOE that will receive magnetic media containing FTI.

I. PERFORMANCE

In the performance of this Agreement between the BOE and the DTS, the Contractor (DTS) agrees to comply with and assume responsibility for compliance by the DTS' employees with the following requirements:

1. All work will be done under the supervision of the DTS or its employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Agreement and except as authorized by federal and state statutory law. Disclosure to anyone other than an officer or employee of the DTS will be prohibited. To the extent that other types of information held by the BOE are open to disclosure under federal or state law, the BOE agrees to provide such information in response to, but not limited to, court orders, Public Records Act requests and investigations by law enforcement authorities. (See Special Terms and Conditions, Exhibit D, number 11.)

3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. The DTS certifies that the data processed during the performance of this Agreement will be completely purged from all data storage components of the DTS' computer facility, and no output will be retained by the DTS at the time the work is completed. If immediate purging of all data storage components is not possible, the DTS certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the BOE's specified designee(s). When this is not possible, the DTS will be responsible for the destruction of the spoilage or any intermediate hardcopy printouts, and will provide to the BOE's specified designee(s) with a statement containing the date of destruction, description of material destroyed and the method used.
6. All computer systems processing, storing, or transmitting Federal tax information must meet the federal standard for security features, Common Criteria for Information Technology Security Evaluation, usually referred to as the Common Criteria, ISO STD 15408. To meet functional and assurance requirements of this standard, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
7. No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
8. The DTS will maintain a list of employees with authorized access. Such list will be provided to the BOE and, upon request, to the IRS reviewing office.
9. The BOE will have the right to void this Agreement if the DTS fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of the DTS to whom returns or return information is or may be disclosed will be notified in writing by the DTS that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as

long as 5 years, or both, together with the costs of prosecution. The DTS shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC §§ 7213 and 7431 and set forth at 26 CFR 301.6103(n).

2. Each officer or employee of the DTS to whom returns or return information is or may be disclosed shall be notified in writing by the DTS that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. The DTS shall also notify such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC §§ 7213A and 7431.
3. Additionally, it is incumbent upon the DTS to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to the DTS by U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

III. INSPECTION

The IRS and the BOE each shall have the right to send its specifically-authorized officers and employees into the offices and plants of the DTS for inspection of the facilities and operations provided for the performance of any work under this Agreement. On the basis of such inspection, specific measures may be required in cases where the DTS is found to be noncompliant with contract safeguards. The DTS agrees to allow an annual site inspection for this purpose by the BOE's specifically-authorized employees and, upon request, by the IRS, and to facilitate an annual site inspection of the Iron Mountain storage facility conducted by the BOE's specifically-authorized employees and, upon request, by the IRS.

CERTIFICATION REQUIREMENTS

4832 Illustration 1

CERTIFICATION OF COMPLIANCE WITH POLICIES

Pursuant to SAM Section 4819.41 and 4832

I hereby certify that I am the agency director or designee; that the matters described herein are in compliance with the criteria and procedures for information technology prescribed in State Administrative Manual (SAM); any acquisitions of new or enhanced information technology capabilities are consistent with project justification approved by Department of Finance, myself or my designee; and that the foregoing statements are true to the best of my knowledge and belief.

Date

Signature and Title
(Specify director or designee)

JUSTIFICATION AND APPROVAL REFERENCE INFORMATION

_____ Finance-Approved FSR	_____ Finance Project #	_____ Approval Date
_____ Agency-Approved FSR	_____ Agency Project #	_____ Approval Date
_____ Workgroup Computing Justification Form (WCJP)	_____ WCJF #	_____ Approval Date
	_____ Project Title	

 X **Data Center IAA** - This is an Interagency Agreement to procure services from a consolidated data center; it involves multiple projects; the funding level is appropriate, and the nature and scope of services to be supplied by the Data Center are consistent with the various approved FSRs and PIERs of this agency; and the required project reporting associated with each active project is current.

SECURITY COMPLIANCE STATEMENT

DTS provides for the integrity and security of customer information assets and complies with the policies as set forth in the State Administrative Manual sections 4840-4845. Entities requesting to connect their networks or their network devices to DTS network or resources accessible on DTS's network, must comply with the following basic information security requirements. These requirements will be included in any Agreement or contract with an entity that includes the provision of connectivity to DTS or a resource accessible on DTS's network.

- A. Firewalls** - This requirement provides a reliable mechanism to help protect DTS and its customers' information and information processing resources from unauthorized access to, and denial/disruption of services or systems.
- **Definition** - A firewall is a computer or system of computers designed to restrict network traffic in order to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, but are strongest when implemented as a hardware/software combination.
 - **Requirements** - Any network used by a customer to connect to DTS information resources will be protected by at least one firewall system properly situated to examine traffic between the network and each external network entry point. The customer shall ensure that firewalls include, at a minimum, provisions for packet filtering, application gateway security mechanisms, and circuit-level gateways.
- B. Physical Security** - This requirement ensures that the hardware that permits network access to DTS Data Center is adequately protected to prevent harm to the physical components that enable connectivity between the customer's network and DTS.
- **Definition** - Physical Security involves measures taken to prevent physical access, which may allow loss of or damage to, the system or the information stored on it.
 - **Requirements** - Physical access to network components, servers, and data storage components used in conjunction with access to DTS information resources should be limited to the appropriate designated staff who implement and maintain the components.
- C. Access Control** - This requirement ensures that policies, procedures and technology mechanisms are in place for DTS's customers only to limit access to the DTS's network and the information resources in DTS's custody to those authorized individuals or entities.
- **Definition** - Access control includes processes and systems to determine which system resources, application functions and information must be restricted to certain customers, business partners, and contractors and to allow access by those customers while preventing access by others.
 - **Requirements** - Access to information designated as private or confidential must be limited to those individuals or entities specifically authorized to access that information. Access to system functions and processes under DTS's custody that can affect the availability, functionality or security of departmental information or information resources should be restricted to those individuals who require that access in order to perform duties essential to the operation and maintenance or use of that system.

DTS is requiring Security Compliance for audit purposes.

- ☒ Customer is in full compliance with the aforementioned security requirements.
- ☐ Customer is not in full compliance, however, will contact DTS's Information Security Officer at (916) 464-3672 to develop a plan of action for compliance with the security requirements.
- ☐ Not Applicable – Customer does not have a network connection to DTS Data Center.

Information Security Officer Signature

Date

SERVICE STANDARDS AND SERVICE LEVEL OBJECTIVES

This document can be viewed on DTS's web page at: www.DTS.ca.gov/resources/slo.pdf